UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/602,167	06/24/2003	Christian Gehrmann	P18116-US1	9436

27045   7590   02/11/2008

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER
TRUONG, THANHNGA B

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
02/11/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04 December 2007*.

2a)☒ This action is **FINAL**.   2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-12* is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All   b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   This action is responsive to the communication filed on December 4, 2007. Claims 1-12 are pending. At this time, claims 1-12 are still rejected.

Response to Arguments

2.   Applicant's arguments filed December 4, 2007 have been fully considered, at least under *35 USC § 101*, but they are still not persuasive. The preamble of claims 10 and 11 contain the phrase, such as "computer readable medium __adapted to configure a processor to communicate__ data message", these claimed languages does not even support anywhere in the specification. In addition the specification recites the language, such as, "**The instructions may be program code means loaded in a memory, such as a RAM, from a storage medium *OR from another computer via a computer network, (emphasis added)*"** (page 5, lines 10-12 of the specification) wherein the code can be transmitted *via a computer network* (e.g., signals, carrier waves, transmissions, optical waves, transmission media) which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claims 10 and 11 recite a non-statutory subject matter.

Applicant's arguments filed December 4, 2007, with respect to the rejection(s) of claim(s) 1-12 under *35 USC § 103* have been fully considered they are not persuasive.

Applicant and/or Applicant's Representative argue that:

The combination of teaching between Graveman and Carman for claims 1-5, 7-12 and the combination of teaching between Graveman, Carman, and Shokrollahi for claims 5-6 are improper.

Examiner respectfully disagrees with Applicant and/or Applicant's Representative and still believes that the combination of teaching between Graveman and Carman teaches the claimed subject matter. In fact, Graveman teaches An approximate message authentication code (AMAC) which, like conventional message authentication codes, provides absolute authentication of the origin of the message, yet

provides an approximate integrity check for the content of the message. The approximate integrity check will be computed probabilistically and will likely be the same for messages having only a small percentage of different bits. A distance measure on the AMACs, such as a Hamming distance measure, may be used to determine whether the number of bit differences between the messages is likely to be within an acceptable amount. The AMAC is a probabilistic checksum based on a shared key. The AMAC uses the message and a shared key as inputs (see abstract of Graveman, and more details of claim 1's limitation are taught by Graveman in column 5, lines 13-40; column 6, line 64 through column 7, line 19; column 8, lines 31-35 of Graveman).

Although Graveman teaches the technique to process message authentication code using initial vectors (which is the symbols of the codeword), Graveman is silent on the capability of showing the details of forming a codeword (e.g., message authentication code or data word) and the tag value to be the selected symbol. On the other hand, Carman teaches codeword in column 2, lines 1-11; column 20, lines 57-67 of Carman, and tag value in Figures 1, 17A-17B and more details in column 3, lines 35-43; column 26, lines 25-36 of Carman. Thus, the combination of teaching between Graveman and Carman teaches the claimed subject matter.

The combination of the teaching between Graveman and Carman further teaches the type of error correction code, wherein Reed-Solomon is one kind of error correcting code which defines in terms of finite field. However they are silent on the capability to show the tag value is an element in a finite field (column 5, lines 37-40 of Graveman). On the other hand, Shokrollahi teaches this limitation (as shown in column 1, lines 19-35 of Shokrollahi). Thus, the combination of teaching between Graveman, Carman, and Shokrollahi teaches the claimed subject matter.

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re

Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, based on the above response, the combination of teaching between Graveman, Carma, and Shokrollahi is proper and efficient.

Graveman, Carma, and Shokrollah do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

Claim Rejections - 35 USC § 101

3.   35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4.   Claims 10 and 11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

a.   _Referring to claims 10-11:_

Claim 10 and 11 recite "a computer program product configured to process a message to determine a tag value from the message and from a key according to a message authentication code." The claim is clearly a software program and it is non-statutory as not being tangibly embodied in a manner so as to be executable. Furthermore, applicant has pointed out in the specification (see lines 6-14 of page 5) "**the following may be implemented in software and carried out in a data processing system or other processing means caused by the execution of computer-executable instructions. The instructions may be program code means loaded in a memory, such as a RAM, from a storage medium or from another computer _via a computer network_. Alternatively, the described features may be implemented by hardwired circuitry instead of software or in combination with**

software", which clearly including intangible media such as signals, carrier waves, transmissions, optical waves, transmission media or other media incapable of being touched or perceived absent the tangible medium through which they are conveyed. Therefore, claims 10 and 11 recite a non-statutory subject matter.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1-5, 7-12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graveman (US 6,851,052 B1), and further in view of Carman et al (US 6,845,449 B1).

      a.   _Referring to claim 1:_

          i.   Graveman teaches a method of processing a message to determine a tag value from the message and from a key according to a message authentication code (column 5, lines 13-30 of Graveman), the method comprising:

          (1)   selecting one of a plurality of symbols (e.g., vectors), the plurality of symbols forming a codeword encoding a data item derived from the message, the codeword encoding the data item according to an error correcting code, wherein said key determines which one of said plurality of symbols is selected; and determining the tag value to be the selected symbol **(column 5, lines 13-40; column 6, line 64 through column 7, line 19; column 8, lines 31-35 of Graveman)**.

          ii.   Although Graveman teaches the technique to process message authentication code using initial vectors (which is the symbols of the codeword), Graveman is silent on the capability of showing the details of forming a codeword (e.g., message authentication code or data word) and the tag value to be the selected symbol. On the other hand, Carman teaches codeword **in column 2, lines 1-**

11; column 20, lines 57-67 of Carman, and tag value in Figures 1, 17A-17B and more details in column 3, lines 35-43; column 26, lines 25-36 of Carman.

      iii.   It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

      (1)   have modified the invention of Graveman (if indeed is not inherently) with the teaching of Carman to authenticating the source and integrity of transmitted or stored information **(column 1, lines 24-25 of Graveman).**

      iv.   The ordinary skilled person would have been motivated to:

      (1)   have modified the invention of Graveman (if indeed is not inherently) with the teaching of Carman to provide absolute authentication of the source or origin of a received message and permits verifying approximate integrity between the original message and the received message **(column 1, lines 28-31 of Graveman).**

      b.   *Referring to claim 2:*

      i.   Graveman further teaches:

      (1)   wherein the data item derived from the message consists of said message **(column 8, lines 29-48 of Graveman).**

      c.   *Referring to claim 3:*

      i.   Graveman further teaches:

      (1)   further comprising determining said data item to be a hash value of a one-way hash function calculated from the message **(column 1, lines 42-45 and line 55 through column 2, line 7 of Graveman).**

      d.   *Referring to claim 4:*

      i.   The combination of the teaching between Graveman and Carman teaches the length of the key **(column 6, lines 44-48 of Graveman),** and Carman further teaches:

      (1)   wherein the key is short enough to be communicated via a user interaction **(column 20, lines 57-67 of Carman).**

      e.   *Referring to claim 5:*

      i.   The combination of the teaching between Graveman and Carman teaches the type of error correction code, wherein Reed-Solomon is one kind of error correcting code **(column 5, lines 37-40 of Graveman),** and Carman further teaches:

      (1)   wherein the error correcting code is a Reed-Solomon code and wherein the tag value is determined by evaluating a Reed-Solomon encoding polynomial at a point determined by the key **(Figure 17B and more details in column 26, lines 3-36 of Carman).**

     f.   _Referring to claim 7:_

      i.   Graveman further teaches:

      (1)   further comprising communicating at least a contribution to the message from a sender to a receiver via a first communications channel **(column 5, lines 36-40 of Graveman);** and communicating the tag value and/or the key from the sender to the receiver via a second communications channel different from the first communications channel **(column 10, lines 16-26 of Graveman).**

     g.   _Referring to claim 8:_

      i.   Graveman further teaches:

      (1)   wherein the second communications channel includes a user interaction **(column 2, lines 11-16 of Graveman).**

     h.   _Referring to claims 9 and 12:_

      i.   These claims consist a communications device for communicating data messages, the communications device to implement claim 1, thus they are rejected with the same rationale applied against claim 1 above.

     i.   _Referring to claims 10 and 11:_

      i.   These claims consist a computer program product configured to process a message to determine a tag value from the message and from a key according to a message authentication code, the computer program product to implement claim 1, thus they are rejected with the same rationale applied against claim 1 above.

7.   Claims 5-6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Graveman (US 6,851,052 B1), in view of Carman et al (US 6,845,449 B1), and further in view of Shokrollahi (US 6,631,172).

  a.   *Referring to claims 5 and 6:*

        i. The combination of the teaching between Graveman and Carman teaches the type of error correction code, wherein Reed-Solomon is one kind of error correcting code which defines in terms of finite field. However they are silent on the capability to show the tag value is an element in a finite field **(column 5, lines 37-40 of Graveman).** On the other hand, Shokrollahi teaches this limitation **(as shown in column 1, lines 19-35 of Shokrollahi).**

        ii. It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:

             (1)   have modified the invention of Graveman-modified (if indeed is not inherently) with the teaching of Shokrollahi to authenticating the source and integrity of transmitted or stored information **(column 1, lines 24-25 of Graveman)**.

        iii.   The ordinary skilled person would have been motivated to:

             (1)   have modified the invention of Graveman-modified (if indeed is not inherently) with the teaching of Shokrollahi to provide absolute authentication of the source or origin of a received message and permits verifying approximate integrity between the original message and the received message **(column 1, lines 28-31 of Graveman)**.

Conclusion

8.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

             Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thanhnga (Tanya) Truong whose telephone number is 571-272-3858.

     If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached at 571-272-3859. The fax and phone numbers for the organization where this application or proceeding is assigned is 571-273-8300.

     Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 571-272-2100.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

TBT
February 8, 2008